

**UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS**

UNITED STATES OF AMERICA	)	
	)	Docket No. 20-cr-10012-IT
	)	
v.	)	
	)	<b><i>LEAVE GRANTED ON 4/26/22</i></b>
	)	<b><i>TO FILE REDACTED MEMO &amp;</i></b>
PAUL BATEMAN	)	<b><i>CERTAIN EXHIBITS UNDER SEAL</i></b>

**DEFENDANT’S MOTION TO RECONSIDER THE COURT’S ORDERS DENYING  
DEFENDANT’S MOTION TO SUPPRESS AND MOTION TO COMPEL**

The defendant, Paul Bateman, moves this Court to reconsider its rulings denying his motion to suppress and his motion to compel. *See* D.E. 76 (Motion to Compel); 106 (Motion to Suppress). Recently, undersigned counsel have been made aware of new information relevant to and supportive of both of Mr. Bateman’s motions. Specifically, counsel have identified several warrant applications and complaints from other districts that are very similar, and in some cases identical, to the warrant application and affidavit issued in Mr. Bateman’s case. *See* Exhibits 1-8. Additionally, independent FOIA litigation in the District of Maryland, unrelated to Mr. Bateman’s case, revealed a case opening document from the FBI dating back to 2017, with language describing a Tor hidden service site that is identical to the description of Website A at issue in this case. *Compare* Exhibit 9 with Motion to Suppress, Exhibit A, at ¶ 15. Counsel have also obtained redacted documents [REDACTED] that indicate not only that United States law enforcement was deeply involved in the investigation of this target website as early as 2016, but also that U.S. law enforcement was working in tandem with foreign law enforcement in that investigation. *See* Exhibits 10-11. Finally, an affidavit filed in another case stemming from the same investigation explains why Agent Squire’s assertions about the Tor network were misleading. *See* Exhibit 13.

This information lends substantial support to Mr. Bateman's arguments that the warrant lacked probable cause, that Agent Squire made material omissions in his affidavit, and that Mr. Bateman is entitled to the discovery he has requested from the government. The documents also undermine the government's persistent claims that Mr. Bateman's arguments are purely speculative. In light of this information, Mr. Bateman moves this Court to reconsider its prior rulings, grant his motion to suppress, order a *Franks* hearing, and grant his motion to compel discovery.

**I. Mr. Bateman's Case is Just One in a Large-Scale, Multi-National, Coordinated Investigation, Which Was Not Disclosed in Agent Squire's Affidavit.**

Undersigned counsel have identified multiple cases from across the country that rely on an August 2019 tip from an undisclosed FLA that an IP address was used to visit a Tor hidden services website sometime in April or May 2019. The number of similar cases using similar, if not identical, language to the search warrant affidavit in Mr. Bateman's case suggests a large-scale, coordinated investigation into websites hosted on the Tor network akin to the Playpen investigation. See "The Playpen Cases: Mass Hacking by U.S. Law Enforcement," Electronic Frontier Foundation, available at <https://www.eff.org/cases/playpen-cases-mass-hacking-us-law-enforcement>. These cases and documents demonstrate that the purportedly individualized and as-yet unsupported FLA "tip" regarding a single IP address referenced in Agent Squire's affidavit was actually part of a much wider investigation than what has been disclosed by the government thus far or by Agent Squire in his affidavit. Furthermore, the scale of the investigation, involving an undisclosed amount of IP addresses, calls into question not just the methodology used to de-anonymize the IP addresses, but the reliability of that as-yet undisclosed methodology.

**II. U.S. Law Enforcement Was Working More Closely and Collaboratively with Foreign Law Enforcement Agencies than Was Previously Disclosed.**

The documents shed new light on the role of U.S. law enforcement in the investigation of [REDACTED] as a collaborative partner of foreign law enforcement agencies. From these new documents, six particular facts stand out.

First, an FBI report dated January 13, 2017 documents a “preliminary investigation” into a Tor hidden service site with language identical to that found on [REDACTED]. This document indicates that the FBI opened an investigation into [REDACTED] more than two years before the IP addresses that had purportedly visited [REDACTED] were transmitted by a foreign law enforcement agency to U.S. law enforcement. *See* January 13, 2017 FD-302, attached as Exhibit 9. Agent Squire withheld this information from his affidavit. Taken with the other facts counsel has since discovered about the extent to which U.S. law enforcement was involved in a joint venture with foreign law enforcement to investigate the website, Agent Squire’s omission is significant.

Second, documents from [REDACTED] connect the Department of Homeland Security, and specifically Special Agent Squire and HSI Boston, to a joint, international investigation of a specific constellation of Tor hidden service sites starting as early as 2016.<sup>1</sup> [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

---

<sup>1</sup> [REDACTED]

Two of those individuals were Patrick Falte and Benjamin Faulkner, the creators and lead administrators of the Giftbox Exchange and Child's Play, two Tor hidden services sites dedicated to the sharing of child abuse materials. *Id.*; see also *United States v. Benjamin Faulkner and Patrick Falte*, Case No. 3:17-CR-00049-JAG (E.D. Va., Oct. 4, 2016) (Criminal Complaint) (attached as Exhibit 12).<sup>2</sup> These individuals were arrested and interviewed in the United States. Ex. 10 at 5; Ex. 12 at ¶ 9. During those interviews with U.S. law enforcement agents, Faulkner or Falte, or both, provided "passwords to devices, ... encryption keys and signature keys." Ex. 10 at 5; see also Ex. 12 at ¶ 9.

HSI shared this information from Faulkner and/or Falte with foreign law enforcement agencies. In particular, HSI immediately sent the usernames, passwords, and encryption keys to the Tor site Child's Play to the Australian police.<sup>3</sup> HSI appears to have also shared the information from these interviews with [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Although the documents from [REDACTED] are heavily redacted, there are multiple references to Homeland Security, as well as HSI Boston and Agent Squire. [REDACTED]

[REDACTED]

---

<sup>2</sup> See also "Four Men Sentenced to Prison for Engaging in a Child Exploitation Enterprise on the Tor Network," Department of Justice (Aug. 12, 2019) (available at <https://www.justice.gov/opa/pr/four-men-sentenced-prison-engaging-child-exploitation-enterprise-tor-network>); Håkon F. Høydal, "Breaking the Dark Net: Why the Police Share Abuse Pics to Save Children," *VG* (Oct. 7, 2017), available at <https://www.vg.no/spesial/2017/undercover-darkweb/?lang=en>.

<sup>3</sup> A special unit in the Australian police called Task Force Argos then ran Child's Play for 11 months. See Høydal, *supra* note 2.

It is clear that the investigation of multiple Tor hidden websites, including [REDACTED], relied heavily on collaboration between U.S. and foreign law enforcement. Canadian, U.S., New Zealand, and Australian law enforcement agencies worked together to investigate, locate, and arrest Faulkner and Falte. *See* Ex. 10 at 1-5; Høydal, *supra* note 2. U.S. law enforcement obtained information from those individuals, and then took that information to foreign law enforcement to continue the investigation into Tor hidden services sites. *Id.* It was only because of that cooperation and collaboration that agents were able to identify and eventually arrest [REDACTED]

Third, one of the attached affidavits states that this investigation of multiple target websites on the Tor network was a “collaborative” effort with foreign law enforcement partners. *United States v. Thomas S. Clark*, Case No. 2:21-MJ-00147-JLW (W.D. Wash., March 11, 2021) (Complaint) (“*Clark* Complaint”) attached as Exhibit 4, at ¶ 5. The *Clark* complaint clearly describes the same investigation that led to the identification of Mr. Bateman’s IP address. Like Mr. Bateman’s case, *Clark* involved a tip from an FLA that a specific IP address accessed a target website on the Tor network in April 2019. *See* Ex. 4, at ¶¶ 5-10. The language of the *Clark* complaint also mirrors that in Agent Squire’s affidavit, especially in its description of the Tor network. *Compare* Ex. 4, ¶ 9, with Motion to Suppress, Exhibit A, ¶¶ 12-13. In both cases, administrative subpoenas were sent to internet services providers (Comcast) at similar times (September 5, 2019 in *Clark*, September 10, 2019 in Mr. Bateman’s case). Ex. 4, ¶ 10; Motion to

Suppress, Exhibit A, ¶ 27. The “collaborative” investigation that formed the basis of the *Clark* case is therefore the same investigation that led to Mr. Bateman’s IP address.

Fourth, the *Clark* Complaint also indicates that *Agent Squire* viewed one of the target websites that was hosted on the server seized by a foreign law enforcement agency in June 2019 **while that website was still operational**. Ex. 4, at ¶ 8. The *Clark* Complaint – written by HSI Special Agent Berg – states that “in June of 2019, a foreign law enforcement agency seized a computer server hosting three ‘dark web’ sites operating on the Tor (The Onion Router) Network.” *Id.* at ¶ 5. The Target Website in the *Clark* case does not appear to be [REDACTED] but does appear to be hosted on the same server as [REDACTED].<sup>4</sup> The complaint goes on to state that HSI was notified by an FLA that an IP address had accessed a target website on April 12, 2019. *Id.* at ¶ 7. It then states, “[a]ccording to the foreign law enforcement agency and HSI Special Agent Greg Squire who observed the TARGET WEBSITE while it was operational, child pornography images and videos were trafficked through the TARGET WEBSITE via the posting of web links within forum messages.” *Id.* at ¶ 8. If Agent Squire were able to view a target website that was hosted on a server seized in June 2019 **while that website was operational**, it would necessarily have been well before U.S. law enforcement received the tip from [REDACTED] in August 2019. Agent Squire omitted the fact that he was involved in the investigation of a particular set of Tor hidden sites prior to the receipt of an FLA “tip” involving the target website from his affidavit. This fact, along with the others revealed in this new set of documents, directly counters the narrative in Agent Squire’s affidavit that U.S. law enforcement simply received a single tip from an undisclosed FLA with no other context.

---

<sup>4</sup> Agent Squire does not indicate when the server hosting [REDACTED] was seized. However, documents in other cases stemming from the same investigation indicate that the server hosting [REDACTED] was seized by an FLA [REDACTED] in June 2019. *See* Ex. 1, at ¶ 14; Motion to Suppress, D.E. 106, at 17.

Fifth, in another case, HSI Boston is noted to have been working in tandem with foreign law enforcement to investigate Tor hidden services sites as early as 2018. *See United States v. Dashawn Webster*, Case No. 2:18-CR-101-RAJ (E.D. Va. May 18, 2018) (Affidavit in Support of Application for Issuance of Criminal Complaint) (“*Webster* Complaint”) attached as Exhibit 8, at ¶ 13 (“HSI Boston is also conducting an investigation of various Darkweb sites **along with** foreign law enforcement partners.”) (emphasis added). In fact, HSI Boston, and Agent Squire in particular, are specifically noted in several cases involving U.S.-FLA joint investigations outside of this District. *See* Ex. 4, at ¶¶ 5-8; Ex. 6, at ¶ 62; Ex. 8, at ¶ 12.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Together, these documents show that U.S. law enforcement's involvement in the investigation of [REDACTED] was much more significant and much more collaborative with foreign law enforcement partners than what was indicated in Agent Squire's affidavit. The materials reveal that U.S. law enforcement became aware of, and began investigating, [REDACTED] as early as 2016, when the website was created. From the outset of the investigation, U.S. law enforcement worked in tandem with foreign law enforcement agencies, including, at the very least, law enforcement in Canada, New Zealand, and Australia. HSI Boston, and Agent Squire in particular, appears to have played a significant role in that investigation. Agent Squire even viewed one of the Tor hidden services websites targeted in this wide-scale investigation while that website was operational, which necessarily had to have occurred months prior to when the [REDACTED] sent the "tips" regarding an as-yet unknown number of IP addresses. [REDACTED]

[REDACTED]

The documents demonstrate that U.S. law enforcement was engaged in a joint venture with foreign law enforcement partners to investigate multiple Tor hidden services websites, including [REDACTED]. Failing to include the extent to which U.S. law enforcement was engaged in a joint venture to investigate the target website in Mr. Bateman's case was a significant and material omission. *See United States v. Valdivia*, 680 F.3d 33, 51 (1st Cir. 2012). This is especially true because, as described below, the new materials further corroborate the use of a network investigative technique (NIT) to de-anonymize a large number of IP addresses.

The documents also demonstrate that there is a significant amount of withheld discovery material to Mr. Bateman's suppression issues. This material includes, but is not limited to, the identity of the country (and agency) that infiltrated the website, the identity of the country (and agency) that seized the server (if different), the identity of the country (and agency) that deployed a technique that identified Mr. Bateman's IP address, the circumstances and methodology of that identification; and the user history and logs [REDACTED]

[REDACTED]. These are some of the items that were specifically requested, and which were denied in this Court's ruling. *See* D.E. 85 (Order Denying Motion to Compel). This material should have been produced in order for the suppression issues to have been decided on a fair and accurate record. This material should now be produced to counsel, pursuant to the protective order issued in this case, or at a minimum should be produced to the Court for an *in camera* inspection.

### **III. The Additional Materials Substantiate Mr. Bateman's Claim that a NIT Was Used.**

The newly discovered materials demonstrate that this case arose from an operation that was massive in scope and involved large numbers of IP addresses. The operation was so large that U.S. law enforcement used boiler-plate affidavits for search warrants that required only minor modifications. The number of cases stemming from the same investigation, and the likely much larger number of IP addresses identified by law enforcement, is further evidence that the investigation involved a NIT, a technique that necessarily interferes with computers wherever they are located. *See* Motion to Suppress, Exhibit H (Murdoch Declaration) at ¶ 23 (noting that a NIT "interferes with a user's computer"); ¶ 31 ("Traffic analysis is extremely unlikely to yield the hundreds of IP addresses submitted by the [redacted] nor give [redacted] the confidence that these IP addresses visited the Onion Service in question"). That calls into serious doubt Agent Squire's

representations in the Affidavit that no U.S. computer was interfered with, especially since that assurance was only made as to the tip-providing FLA, without reference to U.S. involvement at the front end of the investigation and without reference to the server-seizing FLA and/or country.

As the number of cases that have stemmed from this multi-national investigation grow, so too do the number of omissions from Agent Squire's affidavit. The new documents discovered by undersigned counsel demonstrate that Mr. Bateman's claims are not pure speculation. This Court should reconsider its denial of Mr. Bateman's motions to compel discovery and to suppress. The Court should also order a *Franks* hearing and order the government to turn over the discovery that Mr. Bateman has sought.

**IV. Agent Squire's Assertions About the Tor Network, Adopted by this Court in its Order Denying Mr. Bateman's Request for a *Franks* Hearing, Were Misleading.**

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] This Court adopted Agent Squire's conclusions in denying Mr. Bateman's motion for a *Franks* hearing. *See* Order Denying Motion to Suppress, D.E. 117, at 9. For example, the

Court noted that even if Agent Squire had omitted the fact that law enforcement had no information that the internet user associated with Mr. Bateman's IP address had navigated beyond Website A's homepage, "it would not be a material [omission]" because "the effort required to access Website A suggests that an individual visiting the site—even if just the homepage—was actively and willfully seeking out its content." *Id.*

An affidavit recently filed in yet another case stemming from the same investigation directly undermines this conclusion. *See United States v. Stuart*, 21-cr-00007 (W.D.N.Y. Jan. 31, 2022) (Affidavit of Gerald R. Grant) (attached as Exhibit 13). The affidavit, written by an expert in computer forensics, explains that "[w]hile it is true that websites on the Tor network are not directly 'indexed' by search engines - such as Google - in the same manner as websites on the public internet, that does not mean that a user cannot easily find links to hidden Tor websites through Google." Ex. 13 at ¶ 4. The expert affidavit specifically notes that a "simple search" can lead to web pages that contain links to hidden Tor websites. *Id.* at ¶ 5. Therefore, "it is possible for a user to easily find a list of links to hidden Tor websites, click on a link, and be taken to that website **without being aware of what content it contains**. The typical names of these hidden Tor websites do not indicate possible content, due to the use of the 16-or-56-character web address." *Id.* at ¶ 6 (emphasis added).

Respectfully, Mr. Bateman moves this Court to reconsider its conclusion that Agent Squire's omission that the tip did not indicate that an internet user had navigated beyond the homepage of Website A would not have been a material one. The Court's support for that conclusion – that simply navigating to the website means an individual was "actively and willfully seeking out its content," is flawed. The Grant affidavit indicates that an individual could have accessed the homepage of Website A without being aware of its content. Moreover, even if it were

true that an individual did know what Website A contained, a one-time visit to the website's homepage, without any evidence that that individual logged into that website, or viewed any child abuse material on that website, cannot establish probable cause. *See United States v. Falso*, 544 F.3d 110, 120-21 (2d Cir. 2008). That the website in question did not contain any child abuse material on its homepage, and that the government had no evidence that the individual associated with the IP address actually had any log-in credentials for the website further vitiate any probable cause.

### CONCLUSION

For the aforementioned reasons, this Court should reconsider its rulings denying Mr. Bateman's motions to compel and to suppress. The Court should order the government to turn over the discovery requested by Mr. Bateman, suppress the evidence obtained as a result of the search warrant, and order a *Franks* hearing.

Respectfully submitted,  
PAUL BATEMAN  
By His Attorneys,

/s/ Sandra Gant  
Sandra Gant, BBO # 680122  
Federal Public Defender Office  
51 Sleeper Street, 5th Floor  
Boston, MA 02210  
Tel: 617-223-8061

/s/ Caitlin Jones  
Caitlin Jones, MN ID # 0397519  
Federal Public Defender Office  
51 Sleeper Street, 5th Floor  
Boston, MA 02210  
Tel: 617-223-8061

CERTIFICATE OF SERVICE

I, Sandra Gant, hereby certify that this document filed through the ECF system will be sent electronically to the registered participant(s) as identified on the Notice of Electronic Filing (NEF) on April 26, 2022.

/s/ Sandra Gant  
Sandra Gant